Bitcoin Mania

Sue Halpern
JANUARY 18, 2018 ISSUE

Blockchain Revolution: How the Technology Behind Bitcoin Is Changing Money, Business, and the World
by Don Tapscott and Alex Tapscott
Portfolio/Penguin, 348 pp., $30.00

Attack of the Fifty Foot Blockchain: Bitcoin, Blockchain, Ethereum and Smart Contracts
by David Gerard
CreateSpace, 178 pp., $16.95 (paper)

Yoshikazu Tsuno/AFP/Getty Images

James MacWhyte at a bitcoin trading club meeting, Tokyo, February 2014

The first time I bought virtual money, in October 2017, bitcoins, the cryptocurrency everyone by now has heard of, were trading at $5,919.20. A month later, as I started writing this, a single coin sold for $2,000 more. “Coin” is a metaphor. A cryptocurrency such as bitcoin is purely digital: it is a piece of code—a string of numbers and letters—that uses encryption techniques and a decentralized computer network to process transactions and generate new units. Its value derives entirely from people’s perception of what it is worth. The same might be said of paper money, now divorced from gold and silver, or of gold and silver for that matter. Money is a human invention. It has value because we say it does.

In 2008, when a person or persons going by the name Satoshi Nakamoto published the whitepaper “Bitcoin: A Peer-to-Peer Electronic Cash System,” bitcoins were worth nothing because they didn’t exist. Three months later, when the first version of bitcoin software was released by Nakamoto and the inaugural bitcoins were traded, they were essentially free. By September 2010, a single bitcoin cost about six cents. By June 2011, it was $22.59. And while the price had its ups and downs, the overall trend was up, up, up. By the end of 2013, as the idea of a currency controlled exclusively by computers running

cryptographic algorithms created and traded without the intercession of a central bank, a nation-state, a taxation authority, or any kind of regulation began to take hold, especially among libertarians and those unsettled by the financial crisis, as well as among black-market criminals and terrorists, it was nearly $1,000.* The higher the price, the greater the interest of investors and speculators, which propelled the price even higher.

Because the software was programmed to issue a finite number of bitcoins—21 million—bitcoin's spectacular trajectory seemed, and continues to seem, like a textbook case of supply and demand. (Nearly 80 percent have been issued so far through a computer-intensive process called "mining.") How high will the price go? The Internet is full of prognostications—$22,000 by the end of 2018, $50,000 by 2020—that make bitcoin's mid-December valuation at over $18,000 look like a bargain, which, of course, is driving more investment. And this despite warnings of a bitcoin bubble, predictions of a future crash, and an admonishment from Jamie Dimon, the CEO of JPMorgan Chase, who called bitcoin a fraud that will not end well for investors. Still, Dimon conceded that for people who reside in countries with unstable currencies and hyperinflation, like Venezuela or Argentina, bitcoin might be a useful option, as indeed it has turned out to be.

He also acknowledged its utility for the two billion people around the world without access to traditional banking institutions, who are known as "the unbanked." For them, a cell phone can function as a bankbook, a debit card, and a way to send and receive payments. A website called Abra, for example, enables users to send bitcoins, which are denominated fractionally down to eight decimal points, from one mobile phone to another, anywhere in the world; the receiver can keep the payment in bitcoin or exchange it for digital dollars or pesos or some other currency, and spend them at merchants that accept Abra as a payment system.

It gets a little more complicated, though, if the recipient wants to convert the payment into physical cash. Consider the case of an unbanked Filipino woman who has received a remittance from her daughter in Canada. As Don and Alex Tapscott explain in *Blockchain Revolution: How the Technology Behind Bitcoin Is Changing Money, Business, and the World*: "She checks the app and notices there are four other Abra users within a four-block radius of her. She messages them all to see who will exchange her digital pesos for physical pesos and at what price. The four come back to her with different 'bids.'" She then chooses the one with the highest customer satisfaction rating, though not the lowest bid, and meets him to make the exchange.

Using bitcoin as if it were "regular" money to buy things, however, has proved to be more challenging, in part because its value keeps fluctuating, and in part because businesses have been slow to accept it as a form of payment. That may be changing. You can now use bitcoin to pay for a pizza from Domino's or a sandwich from Subway, a subscription to the *Chicago Sun- Times* or the Dish Network, a couch (and anything else on its site) from

Overstock, a gallon of maple syrup from a small sugarhouse in Vermont, or airline tickets on a number of carriers—and the list is growing.

My own cryptocurrency exchange experience was more mundane than that of the woman in the Philippines. I logged onto a website called Coinbase and created an account linked to my credit card. Coinbase gave me the option of buying three different digital currencies: bitcoin, ether, or litecoin. Since the $50 I was willing to invest was more than ten times less than the cost of a single bitcoin even before Coinbase subtracted its service fee, I figured the fractional amount of bitcoin I'd be buying—something on the order of .0076—would hardly be worth it. (Full disclosure: I was wrong.) So instead of bitcoin, I bought .16 ether, and in November 2017, my $50 was up to about $54. But if I cashed out then, Coinbase's fees to do so would have lowered the amount close to my original stake.

These days, transaction fees on cryptocurrency in general, and bitcoin specifically, can be fairly steep. The irony here is that digital currency has been championed as offering more value than traditional money because it moves directly from person to person without the interference of extractive intermediaries like banks and other financial institutions. In theory, that is how peer-to-peer networks are supposed to work. But as more and more money has poured into digital currencies, those banks and financial institutions have begun to move in.

Coinbase, for example, which now has more accounts than the legacy brokerage Charles Schwab, began as a Silicon Valley start-up aimed at making the process of buying and selling cryptocurrencies as easy as online banking. It has received investments from major venture capital funds—Andreessen Horowitz, Union Square Ventures, and DFJ, among others—as well as from the New York Stock Exchange and a number of traditional banks. Those investments have further driven the ever-increasing value of cryptocurrencies. So has—thus far—the ancillary market in bitcoin futures, which opened for trading in mid-December 2017.

While this is arguably how markets are supposed to work, the booming trade in bitcoin has made things difficult for the bitcoin operating system, which is having trouble processing the high volume of transactions coming its way. What began as a structural feature of bitcoin software—that only one-megabyte blocks of transaction data (currently 2,200 to 2,500 transactions on average) could be processed every ten minutes—has become a structural obstacle, as transactions get bottlenecked and the speed at which new ones can be resolved slows to a crawl. One day this past December, for instance, traffic in bitcoin was so overwhelming that many Coinbase account holders were unable to log into their accounts.

Even when it is working smoothly, the bitcoin network is only able to process seven transactions per second. By contrast, PayPal processes 193, and Visa 1,667. If there is any

chance of bitcoin becoming a commercially viable method of payment, it will have to scale up. But scaling up will require a structural change, and since bitcoin software is an open source project with no central authority, amendments to it are ceded to the voluntary developer community. So far, numerous solutions to the scalability issue have been debated, but no consensus has emerged.

The central obstacle to a fully automated monetary system run exclusively by computers is validation: how to ensure that the transactions on the network are legitimate. The bitcoin software devised by Nakamoto employs a number of features to deal with this. The first is basic encryption. A bitcoin is nothing more than a record of value—you have seven bitcoin, I have five bitcoin, and so on—encoded and stored on the bitcoin system as an address. To release that bitcoin to buy something or to cash it out, its owner must use a private encryption key, known only to him or her, which is associated with that account. Matching the private key with the address is done automatically by the decentralized network of computers. If they don't match up, or if the owner of the private key is attempting to spend his or her bitcoin more than once, the computers reject the transaction.

The "miners" who verify and collect these transactions into a block—"miners" being a term for those who run the computers on the network—are also required by the bitcoin software to perform an additional validating function before the block can be added to the bitcoin ledger. Called "proof of work," it is essentially a computational lottery in which all the mining computers vie to guess an algorithmically generated number between zero and 4,294,967,296 with the correct number of zeros preceding it. Finding the target number takes trillions of guesses and a tremendous amount of computing power.

The idea behind "proof of work," according to Daniel Krawisz, of the Satoshi Nakamoto Institute, is that it is "an added complication, like a ritual, so as to make blocks more difficult to generate…. [It] is…a means for a group of self-interested people, none of whom is subordinate to any other, to establish a consensus against a considerable incentive to resist it." Because it takes so much computing power to find this number, miners are motivated to ensure that the transactions they are processing are valid and nonconflicting. But they are motivated to participate in the first place because the software generates a reward: the miner who finds the "proof of work" number first is paid in (an algorithmically determined number of) bitcoins. Though that is how new bitcoins are created, or "mined," and added to the system, as the Tapscotts point out, mining is

> an awkward analogy because it conjures images of experts whose talent might confer some competitive advantage…. It doesn't. Each miner is running the software like a utility function in the background, and the software is doing all the computations…. There's no skill involved.

When the bitcoin network began operating in 2009, people could run the validation program on their personal computers and earn bitcoins if their computer solved the puzzle first. As demand for bitcoin increased, and more people were vying to find the random, algorithmic proof of work validation number, speed became essential. Mining began to require sophisticated graphics cards and, when those proved too slow, special, superfast computers built specifically to validate transactions and mine bitcoins. Individual miners have dropped out for the most part, and industrial operators have moved in. These days, mining is so computer-intensive that it takes place in huge processing centers in countries with low energy costs, like China and Iceland. One of these, in the town of Ordos, in Inner Mongolia, has a staff of fifty who oversee 25,000 computers in eight buildings that run day and night. A company called BitFury, which operates mining facilities in Iceland and the Republic of Georgia and also manufactures and sells specialized, industrial processing rigs, is estimated to have mined at least half a million bitcoins so far. At today's price, that's worth around $7.5 billion.

Still, it's not exactly free money. Marco Streng, the cofounder of Genesis Mining, estimates that it costs his company around $400 in electricity alone to mine each bitcoin. That's because bitcoin mining is not only computationally intensive, it is energy-intensive. By one estimate, the power consumption of bitcoin mining now exceeds that of Ireland and is growing so exponentially that it will surpass that of the entire United States by July 2019. A year ago, the CEO of BitFury, Valery Vavilov, reckoned that energy accounted for between 90 and 95 percent of his company's bitcoin-mining costs. According to David Gerard—whose new book, *Attack of the Fifty Foot Blockchain*, is a sober riposte to all the upbeat forecasts about cryptocurrency like the Tapscotts'—"By the end of 2016," a single mining facility in China was using "over half the estimated power used by *all* of Google's data centres worldwide at the time."

One way bitcoin miners offset these costs is by collecting the very thing digital money, traded peer-to-peer, was supposed to make obsolete: transaction fees. By one estimate, these fees have risen 1,289 percent since March 2015. On any given day, the fees will be in the millions of dollars and now cost upward of twenty dollars per transaction. While transaction fees are not mandatory, they are a way for users to attempt to jump the queue in a system rife with bottlenecks, since those who offer miners a fee to have their transactions included in a block have a better chance of that happening. With so many transactions lined up, waiting to be processed, miners have discretion over which will make it to the head of the line; the higher the fee, the more likely it is to be chosen. As the explanatory website Unlock Blockchain puts it: "when miners mine a block, they become temporary dictators of that block. If you want your transactions to go through, you will have to pay a toll to the miner in charge…. The higher the transaction fees, the faster the miners will put [the transactions] up in their block." As a consequence, transactions can be held up for hours or days or dropped altogether.

Bitcoin's high transaction fees and slow transaction times were two of the reasons I chose to buy ether. But there was another reason as well: while bitcoin was invented to bypass traditional currency by tendering a new kind of money, ether, another cryptocurrency that can be bought, sold, and used to purchase goods and services, was created to raise capital to fund a project called the Ethereum network. The principals behind it are building out what is being trumpeted as the next iteration of the Internet, Web 3.0, also known as "the blockchain."

Thomas Nast

A blockchain is, essentially, a way of moving information between parties over the Internet and storing that information and its transaction history on a disparate network of computers. Bitcoin, for example, operates on a blockchain: as transactions are aggregated into blocks, each block is assigned a unique cryptographic signature called a "hash." Once the validating cryptographic puzzle for the latest block has been solved by a mining computer, three things happen: the result is timestamped, the new block is linked irrevocably to the blocks before and after it by its unique hash, and the block and its hash are posted to all the other computers that were attempting to solve the puzzle. This decentralized network of computers is the repository of the immutable ledger of bitcoin transactions. As the Tapscotts observe, "If you wanted to steal a bitcoin, you'd have to rewrite the coin's entire history on the blockchain in broad daylight."

While bitcoin operates on a blockchain, it is not *the* blockchain. The insight of Vitalik Buterin, the young polymath who created Ethereum, was that in addition to exchanging digital money, the blockchain could be used to facilitate transactions of other kinds of digitized data, such as property registrations, birth certificates, medical records, and bills of lading. Because the blockchain is decentralized and its ledger immutable, those transactions would be protected from hacking; and because the blockchain is a peer-to-peer system that lets people and businesses interact directly with each other, it is inherently more efficient and also cheaper than systems that are burdened with middlemen such as lawyers and regulators.

A company that aims to reduce drug counterfeiting is using the blockchain to follow pharmaceuticals from provenance to purchase. Another outfit is doing something similar with high-end sneakers. Yet another start-up, this one called Paragon, is currently raising money to create a blockchain that "registers everything that has happened to a cannabis product, from seed to sale, letting consumers, retailers and the government know where everything came from." "We are treating cannabis as a normal crop," Paragon's founder

and CEO Jessica VerSteeg, a former Miss Iowa, told a reporter for the website Benzinga. "So, the same way that you would want to know where the corn on your table came from, or the apple that you had at lunch came from, you want to know where the weed you're consuming came from."

While a blockchain is not a full-on solution to fraud or hacking, its decentralized infrastructure ensures that there are no "honeypots" of data available for criminals to exploit. Still, touting a bitcoin-derived technology as the answer to cybercrime may seem a stretch in light of the high-profile—and lucrative—thefts of cryptocurrency over the past few years. Gerard notes that "as of March 2015, a full third of all Bitcoin exchanges"—where people stored their bitcoin—"up to then had been hacked, and nearly half had closed." There was, most famously, the 2014 pilferage of Mt. Gox, a Japanese-based digital coin exchange, in which 850,000 bitcoins worth $460,000,000 disappeared. Two years later another exchange, Bitfinex, was hacked and around $60 million in bitcoin was taken; the company's solution was to spread the loss to all its customers, including those whose accounts had not been drained. Then there was the theft via malware of $40 million by a man in Pennsylvania earlier this year. He confessed, but the other thieves slipped away, leaving victims with no way to retrieve their funds.

Unlike money kept in a bank, cryptocurrencies are uninsured and unregulated. That is one of the consequences of a monetary system that exists—intentionally—beyond government control or oversight. It may be small consolation to those who were affected by these thefts that neither the bitcoin network nor the Ethereum network itself has been breached, which perhaps proves the immunity of the blockchain to hacking. (In 2016, there was a $60 million hack of a company running on the Ethereum system, but the theft occurred because there was a bug in that company's software.)

In addition to demonstrating that a blockchain could be used to build out new ventures, Buterin also showed that those new ventures could be financed, like the Ethereum Network, by the crowd-funded sale of their own branded cryptocurrency. So, for example, Paragon created its own digital "coin," ParagonCoin, and put 100,000,000 up for sale at $1 per coin (to be paid in cryptocurrency). ParagonCoins can be traded for services, once the business is operational—whenever that is—or traded for crypto- and other currencies.

In addition to Jessica VerSteeg, Paragon is fronted by Jayceon Taylor, who is better known in some circles as the rapper The Game. Celebrity promoters like Taylor have become routine in this world of ICOs—initial coin offerings. The boxer Floyd Mayweather is the face of Stox, an ICO that raised $30 million for a service that is supposed to predict sports scores, stock prices, and even the weather. (It appears unable to predict when Stox itself might be up and running.) Another rapper, Ghostface Killah, of the Wu-Tang Clan, is the chief branding officer for Cream Capital, a company that is looking for $30 million to

become the world's largest distributor of cryptocurrency ATMs. Cream Capital got its name from Wu-Tang's 1993 hit "C.R.E.A.M.," which stands for "cash rules everything around me." It's now been repurposed to mean "crypto rules everything around me."

For the moment—and until either the Securities and Exchange Commission decides that ICOs are illegal or investors become wary of tossing money at projects that do not exist and may never exist—crypto, in the form of ICOs, does seem to rule start-up funding; as of this past summer more money has been raised from these crowd-sourced coin offerings than from established venture capital funds and angel investors.

Writing in *The New York Times*, Nathaniel Popper tells of a group of coders in the Bay Area who raised $35 million in under thirty seconds for a proposal to create an ad-free Web browser, and a Swiss team that received $100 million to develop an online chat program. According to the website CoinDesk, as of this fall, more than $3.5 billion has been invested in ICOs, almost all of it in 2017, with close to $3 billion pouring in between June and the end of October. "It's kind of like when you are a little kid and you know you are getting away with something," an investment analyst named Chris Burniske told Popper. "It's not going to last forever, but it's fun in the interim. The space is giddy right now."

Vitalik Buterin's other innovation was to show how smart contracts could be written and stored on the blockchain. These are covenants, written in code, that specify the terms of an agreement. They are "smart" because as soon as its terms are met, the contract executes automatically, without human intervention. Once triggered, it can't be amended, tampered with, or impeded. A writer for the Foundation for Economic Education calls this "programmable money":

> A smart contract is a tool for changing the world. We have this mental model of all these computers synced together. Now imagine that rather than syncing a transaction…we sync software…. Every machine in the network runs the same small program. It could be something simple, like a loan: I send you some money, and your account automatically pays it back, with interest, a few days later…. We all agree to these terms, and it's locked in using the smart contract. We have achieved programmable money. You might say that this doesn't sound very complicated or impressive, but just wait and see where this goes.

Where it might go is anyone's guess, but there is no doubt that smart contracts and the blockchain itself augment the trend toward automation, though it is automation through lines of code, not robotics. For businesses looking to cut costs, this is one of the main attractions of blockchain technology. "If contracts are automated, then what will happen to traditional firm structures, processes, and intermediaries like lawyers and accountants?" ask Marco Iansiti and Karim Lakhani in the *Harvard Business Review*. "And what about

managers? Their roles would all radically change." Indeed. Most blockchain advocates imagine them changing so radically as to disappear altogether, taking with them many of the costs currently associated with doing business. According to a report from the research arm of the Spanish bank Santander, the blockchain "could reduce banks' infrastructure costs attributable to cross-border payments, securities trading, and regulatory compliance by $15–20 billion per annum by 2022."

"Whereas most technologies tend to automate workers on the periphery doing menial tasks," the Tapscotts quote Buterin saying, "blockchain automates away the center. Instead of putting the taxi driver out of a job, blockchain puts Uber out of a job and lets the taxi drivers work with the customer directly." Forget for a moment that this sounds a lot like standing on a street corner and hailing a livery cab: what Buterin is talking about is actually something potentially revolutionary, as the Tapscotts suggest in their title. Whether it will be a revolution for good or one that continues what has come to seem technology's inexorable, crushing ascendance will be determined not only by where it is deployed, but how.

The CIA (through its venture capital group, In-Q-Tel), the defense contractor Northrop Grumman, NASDAQ, Deloitte, Toyota, UnitedHealth, Fidelity, IBM, Credit Suisse, Goldman Sachs, Microsoft, and even JPMorgan Chase, to name just a few, are all looking to employ blockchain technology. So are UNICEF, the Indian state of Andhra Pradesh, and the charity Mercy Corps. The Tapscotts imagine that the blockchain could be used by NGOs to eliminate corruption in the distribution of foreign aid by enabling funds to move directly from giver to receiver. But they also envision it as a way for banks to operate without external oversight, encouraging other kinds of corruption. Either way, we'd be wise to remember that technology is never neutral. It is always endowed with the values of its creators. In the case of the blockchain and cryptocurrency, those values are libertarian and mechanistic; trust resides in algorithmic rules, while the rules of the state and other regulatory bodies are viewed with suspicion and hostility.

Both the Ethereum and bitcoin blockchains are public: anyone can see their ledgers of transactions. For this reason, they are called "permissionless." The ledger doesn't reveal who purchased what by name, but does show what was purchased and when it was purchased and by which encrypted pseudonym. While this is a security feature of a permissionless blockchain, it has also proved to be a boon to law enforcement. The FBI was able to catch Ross Ulbricht, the mastermind of Silk Road—the multimillion-dollar criminal enterprise he operated on the dark web through which users could exchange drugs and guns and stolen goods for bitcoin—because after seizing his computer, they were able to link him to the bitcoin wallets where he stored his earnings. They then used the ledger to trace his entire transaction history.

Ulbricht is now serving a sentence of life without possibility of parole, and the criminals and terrorists who, before his arrest, had relied on bitcoin to shield their identities are using tumblers—programs that mix transactions and make them hard to link to a specific account—or they have migrated to cryptocurrencies that promise full anonymity, which neither the bitcoin nor Ethereum network does.

Just as criminals want to shield their identities on the blockchain, corporations and other institutions are wary of putting proprietary information on a permissionless network. Instead, companies have been exploring how to adapt the blockchain for business, creating invitation-only, "permissioned" peer-to-peer networks that enable speed and efficiency (often by eliminating jobs and bypassing regulation), security, and immutability, while discarding the public and energy-intensive aspects of the original version of blockchain technology.

Last May, the R3 consortium—an association of major banks and financial services companies including ING, Barclays, UBS, Wells Fargo, and the Bank of Canada, as well as the government of Singapore—announced that it had raised $107 million to develop commercial (gated) blockchain applications. And Goldman Sachs has patented its own cryptocurrency, SETLcoin, to digitize and trade real-world assets such as property deeds and stocks on a blockchain. According to Goldman's patent application, these assets will be verified by a trusted third party, such as the Securities and Exchange Commission.

There is no better illustration of the propagation and acceptance—which is to say, co-optation and perversion—of Satoshi Nakamoto's idea of a peer-to-peer, decentralized blockchain trading network, born out of the 2008 financial crisis and an inherent distrust of banks and governments, than a cryptocurrency patent held by an investment bank that relies on an official, third-party regulatory agency for authentication.

Meanwhile, at press time, my $50 of ether was up to $130, and Nakamoto's creation was trading at over $15,000. It took nearly five years for the value of a bitcoin to rise from $0 to $1,000; it had taken five hours for it to move from $15,000 to $16,000. This is not typically how money appreciates. Yet bitcoin is anything but typical. It is computer code in which people have invested *the idea* of value. When that idea, which by now has morphed into the belief that it's possible to get filthy rich out of thin air, no longer captures the public imagination—if the bubble bursts—the blockchain will persist. As those who actually control the flow of money—the banks and corporations and governments—know, that is where the real value of Nakamoto's invention lies.

—December 21, 2017

---

* See www.buybitcoinworldwide.com/price. ↩